

What is Claimed is:

1           1. A method for encryption of digital data for transmission from a transmitter to  
2 a receiver, comprising the steps of:

- 3           a)           providing digital data to a transmitter;  
4           b)           performing XOR masking of the digital data with an XOR mask to  
5                        produce masked digital data;  
6           c)           scrambling the masked digital data using a scrambling formula to  
7                        produce encrypted digital data; and  
8           d)           transmitting the encrypted digital data to a receiver.

1           2. The method of claim 1, wherein subsequent to step (a) and prior to step (b),  
2 the method further comprises the step of  
3                        performing transition controlled encoding of the provided digital data to  
4 produce encoded digital data, such that step (b) XOR masks the encoded digital data to  
5 produce masked digital data.

1           3. The method of claim 2, wherein subsequent to XOR masking step (b) and  
2 prior to scrambling step (c), the method further comprises the step of  
3                        DC balancing the masked digital data to produce DC balanced, masked  
4 digital data, such that step (c) scrambles the DC balanced, masked digital data to  
5 produce encrypted digital data.

1           4. The method of claim 3, wherein the method further comprises the step of

009250-11867560

2 breaking the digital data up into at least a first portion and a second portion and  
3 wherein steps (a) to (c) are performed for the first portion and for the second portion of  
4 the digital data.

1 5. The method of claim 3, wherein the digital data is digital video data  
2 comprising pixel data sets, and steps (a) to (c) are performed for each pixel data set.

1 6. The method of claim 4, wherein prior to step (b), the method further  
2 comprises the steps of

3 i) exchanging a master key between the transmitter and the receiver; and

4 ii) deriving from the master key a first slave key for the first portion of data, and  
5 a second slave key for the second portion of data.

1 7. The method of claim 6, wherein prior to step (b) and subsequent to step (ii),  
2 the method further comprises the step of

3 selecting first and second XOR masks based on information obtained from the  
4 first and second slave keys, respectively, the first and second XOR masks for  
5 performing the XOR masking of step (b) on the first and second portions of data,  
6 respectively.

1 8. The method of claim 6, wherein subsequent to step (ii) and prior to step (c),  
2 the method comprises the step of

3           selecting first and second scrambling formulas based on information obtained  
4   from the first and second slave keys, respectively, the first and second scrambling  
5   formulas for performing the scrambling of step (c) on the first and second portions of  
6   digital data, respectively.

1           9. The method of claim 6, wherein the step of deriving first and second slave  
2   keys from the master key comprises the steps of

3           selecting M bits of the master key as initial values for a M-bit LFSR;

4           selecting a LFSR configuration based on N bits of the master key; and

5           using the selected LFSR configuration and the M-bit LFSR to derive first and  
6   second slave keys.

1           10. The method of claim 8, wherein the M-bit LFSR is a 32-bit LFSR.

1           11. The method of claim 7, wherein the XOR masks are XOR masks that  
2   preserve the TMDS code space.

1           12. The method of claim 8, wherein the scrambling formulas are scrambling  
2   formulas that preserve the TMDS code space.

1           13. An apparatus for encryption of digital data for transmission from a  
2   transmitter to a receiver, the apparatus comprising  
3   a communication link having a first end and a second end,

4 a video transmitter coupled to the first end of the communication link, the video  
5 transmitter comprising  
6 means for receiving digital data;  
7 transition controller for performing transition controlled encoding  
8 of the provided digital data to produce encoded digital data.  
9 XOR mask logic for performing XOR masking of the encoded  
10 digital data with an XOR mask to produce masked digital data;  
11 DC balancing logic for DC balancing the masked digital data to  
12 produce DC balanced, masked digital data;  
13 scrambling logic for scrambling the DC balanced, masked digital  
14 data using a scrambling formula to produce encrypted digital data; and  
15 means for transmitting the encrypted digital data; and  
16 a video receiver coupled to the second end of the communication link for  
17 receiving the encrypted digital data.

1 14. The apparatus according to claim 13, wherein the apparatus further  
2 comprises

3 means for breaking up the digital data into at least a first portion and a second  
4 portion and wherein the apparatus operates on the first portion and on the second portion  
5 of the digital data.

1 15. The apparatus according to claim 13, wherein the apparatus further  
2 comprises

3 means for breaking the digital data into pixel data sets, and wherein the apparatus  
4 operates on each pixel data set.

1 16. The apparatus according to claim 14, wherein the apparatus further  
2 comprises

3 means for exchanging a master key between the transmitter and the receiver; and

4 means for deriving from the master key a first slave key for the first portion of  
5 data, and a second slave key for the second portion of data.

1 17. The apparatus according to claim 16, wherein the apparatus further  
2 comprises

3 means for selecting first and second XOR masks based on information obtained  
4 from the first and second slave keys, respectively, the first and second XOR masks being  
5 used by the XOR masking means for XOR masking the first and second portions of data,  
6 respectively.

1 18. The apparatus according to claim 16, wherein the apparatus further  
2 comprises

3 means for selecting first and second scrambling formulas based on information  
4 obtained from the first and second slave keys, respectively, the first and second  
5 scrambling formulas being used by the scrambling means for scrambling the first and  
6 second portions of digital data, respectively.

1           19. The apparatus according to claim 16, wherein said means for deriving from  
2 the master key a first slave key for the first portion of data, and a second slave key for  
3 the second portion of data comprises

4           means for selecting M bits of the master key as initial values for a M-bit LFSR;

5           means for selecting a LFSR configuration based on N bits of the master key; and

6           means for using the selected LFSR configuration and the M-bit LFSR to derive  
7 first and second slave keys.

1           20. A method for encryption in a high-speed digital video transmission system,  
2 the method comprising the steps of:

3           a)       performing transition controlled encoding of a first sequence of n bit  
4 data words into encoded n+1 bit data characters where the n is a  
5 positive integer,

6           b)       DC balancing the encoded n+1 bit data characters to produce DC  
7 balanced, masked n+2 bit data characters;

8           c)       encoding control data into encoded n+2 bit control characters,

9           d)       encrypting the encoded n+2 bit control characters to produce n+2 bit  
10 encrypted control characters,

11          e)       generating a serial data stream in response to the encrypted data  
12 characters and encrypted control characters, and

13          f)       transmitting the serial data stream over a communication link.

- 1           21. The method of claim 20, wherein the step of encrypting the encoded  $n+2$  bit
- 2   control characters comprises the step of
- 3           including information regarding the timing of transmission of another encoded
- 4   control character in the encoded  $n+2$  bit control characters.

009250-11862500